O E JOJO E

METHOD AND APPARATUS FOR IMPLEMENTING PROCESSOR INSTRUCTIONS FOR ACCELERATING PULIC-KEY CRYPTOGRAPHY Sheueling Chang Shantz, et al. 10/626,420

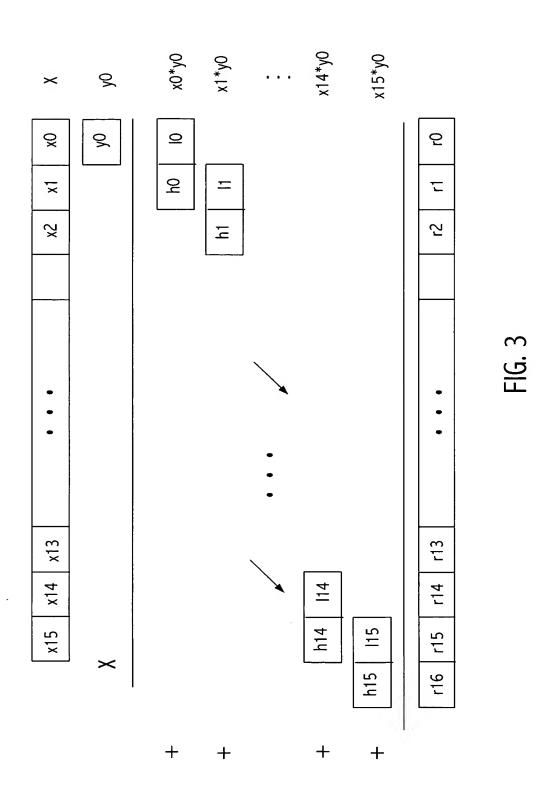
N N N N N N N N N N N N N N N N N N N	>₌	λ\	>_			0	1/35	0		0			
	X ARRAY	Y ARRAY	P ARRAY		yo * X	n0 * P	y1 * X	n1 * P	y15 * X	n15 * P	1		
	0x	δ,	0x									0	
	×	y1	×									0	
	x2	y2	x2									•	
												•	
							_					0	
	•				•							0	
	•	-	•		•	•	-	•					
							-	•					
	-												
	x13	y13	p13										
	x14	y14	p14								i.		
	x15	y15	p15						-	•		•	
		×	MOD						•	•		•	
			~										
		_									·		
	FIG 1	5											
					+	+	+	+	+	+			



	x15	x14	x13	• • •	x2	x1	хО
+	y15	y14	y13	• • •	x2	х1	хО
-							
s16	s15	s14	s13	• • •	s2	s1	s0

FIG. 2





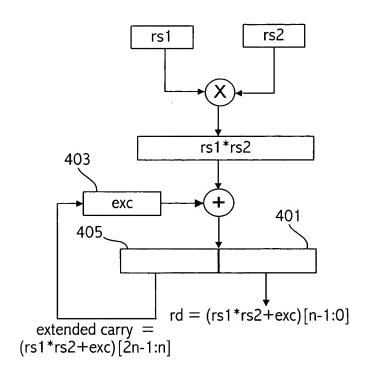


FIG. 4A

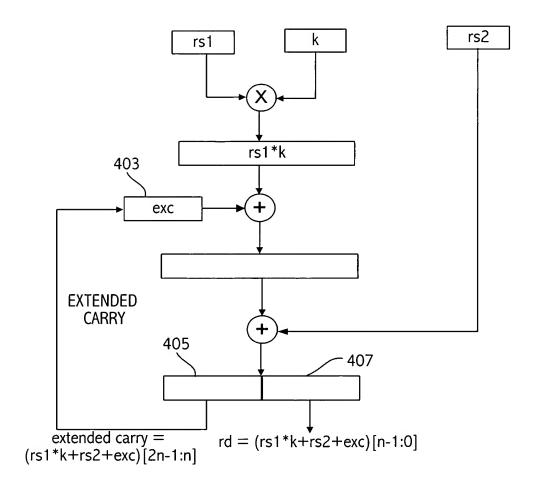


FIG. 4B

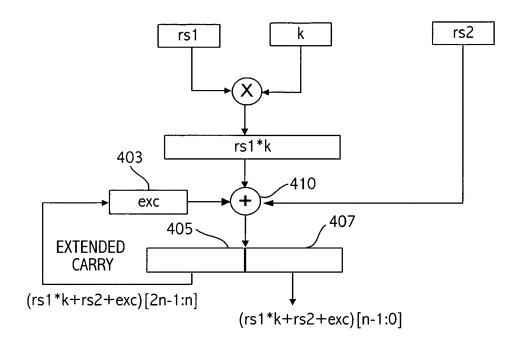
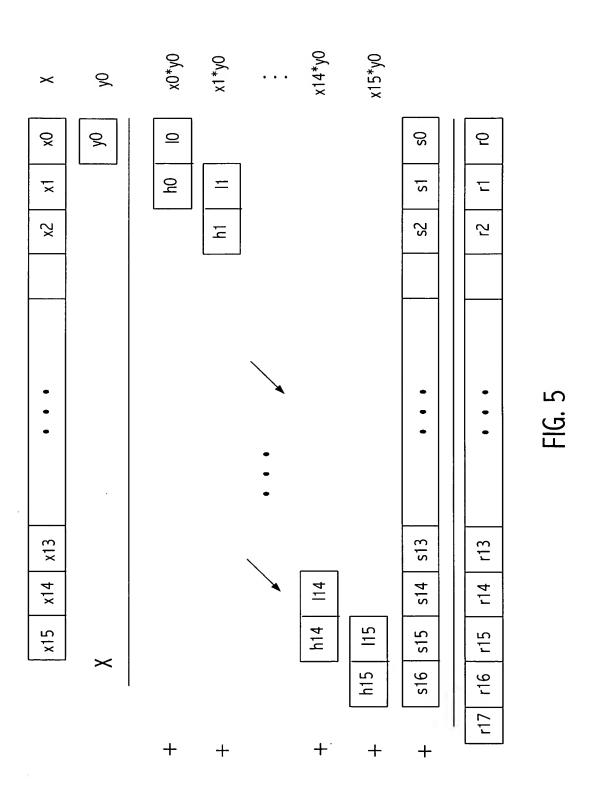


FIG. 4C



8/35

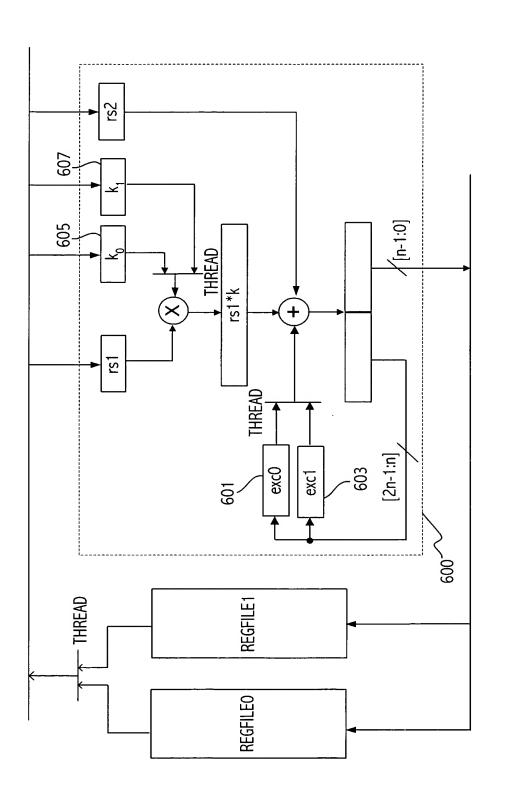


FIG. 6

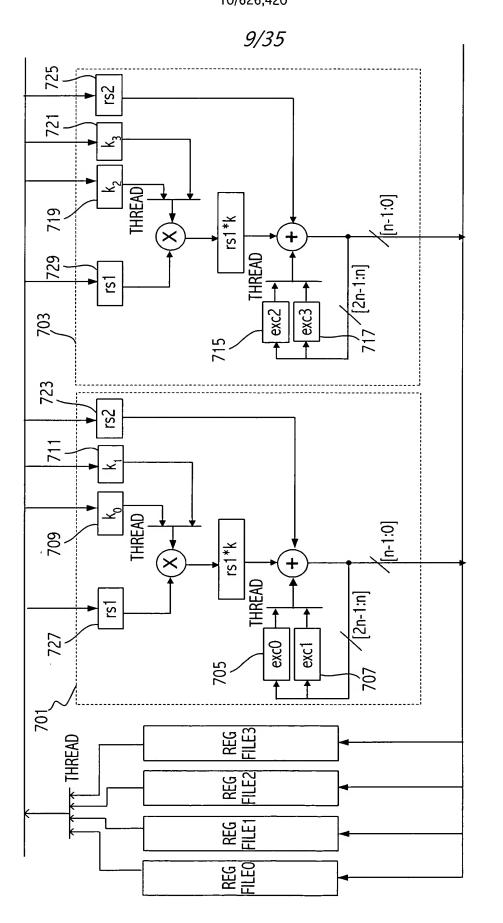


FIG 7

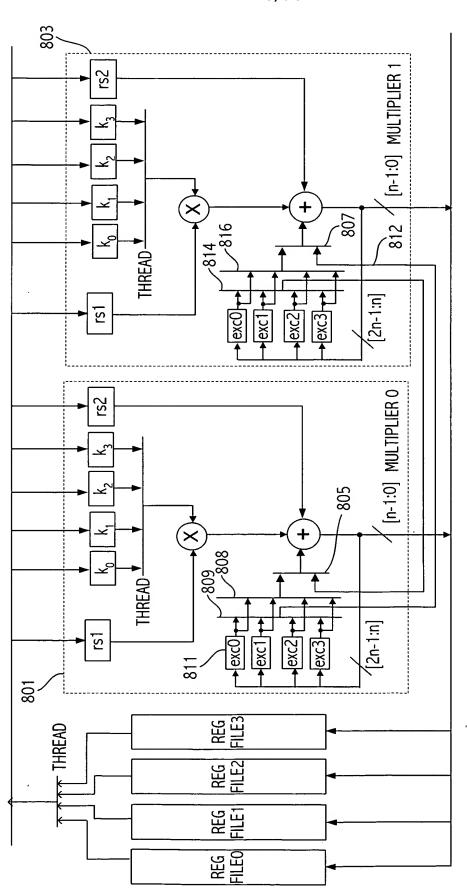


FIG. 8

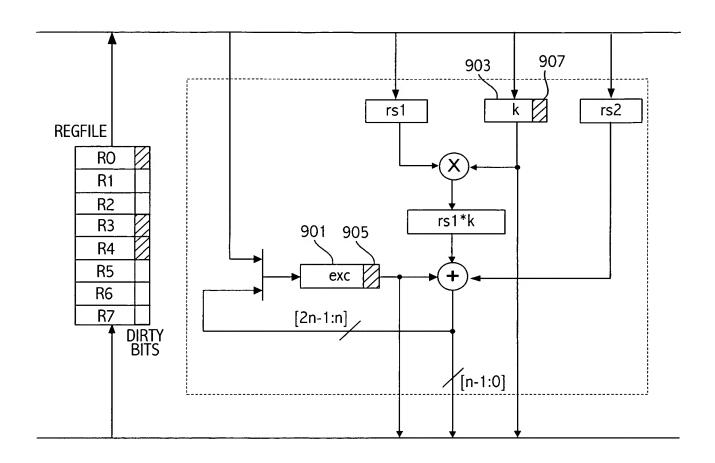


FIG. 9

12/35

FIG. 10

FIG. 11

FIG. 12

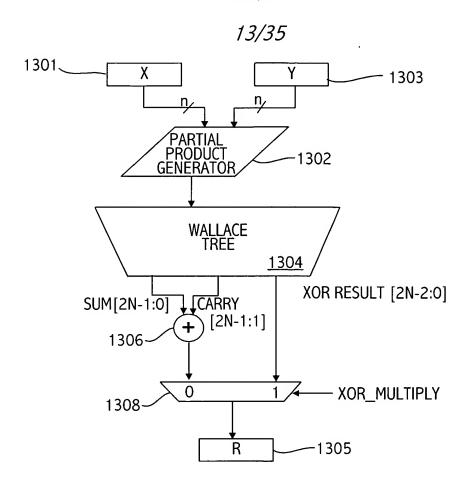


FIG. 13

		1	~SF	1 F8	~SD -SE F7	SD E8 F6	SD E7 F5	D8 E6 F4	D7 E5 F3	D6 E4 F2	D5 E3 F1	D4 E2 F0	D3 E1	D2 E0 SE	D1	D0 SD
1	-SG H7	G8 H6	G7 H5	G6 H4	G5 H3	G4 H2	G3 H1	G2 H0	G1	GO SG		SF		5 2		
C16	C16	C16	C16	C16	C16	C16	C16	C16				S12 C12 Z4		_	S9 C9 Z1	S8 C8 Z0
C16	S15 C15		S13 C13	S12 C12	S11 C11	S10 C10	S9 C9	S8 C8	S7 C7	S6 C6	S5 C5	S4 C4	S3 C3	S2 C2	S1 C1	S0 C0

WITH [S7:S0] AND [C7:C0] GOING TO THE CARRY LOOK-AHEAD ADDER.

FIG. 12B

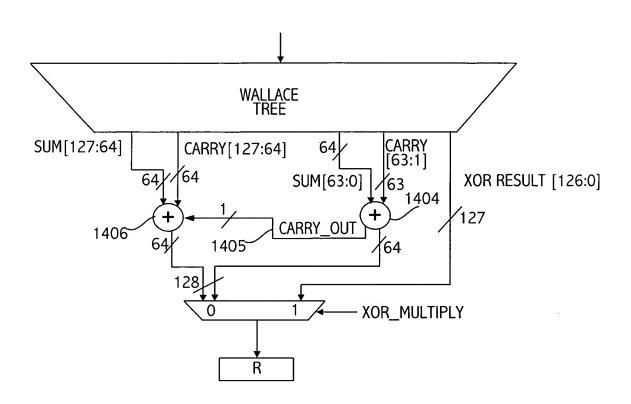


FIG. 14

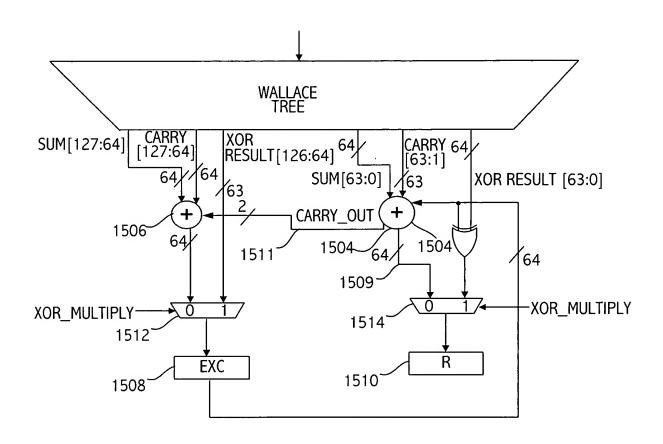


FIG. 15

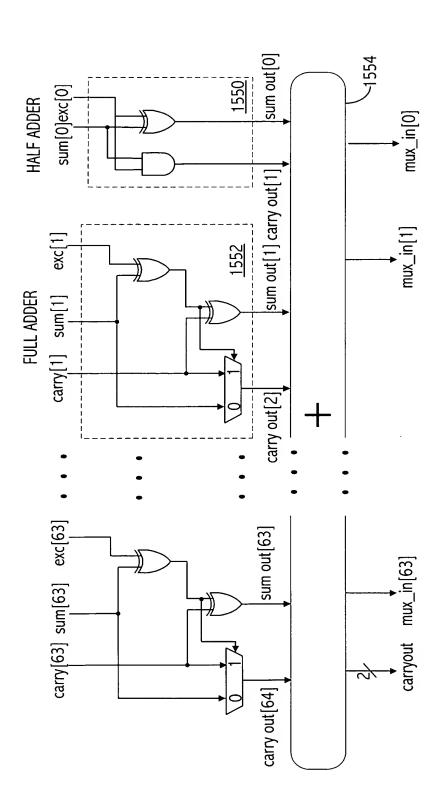


FIG. 15a

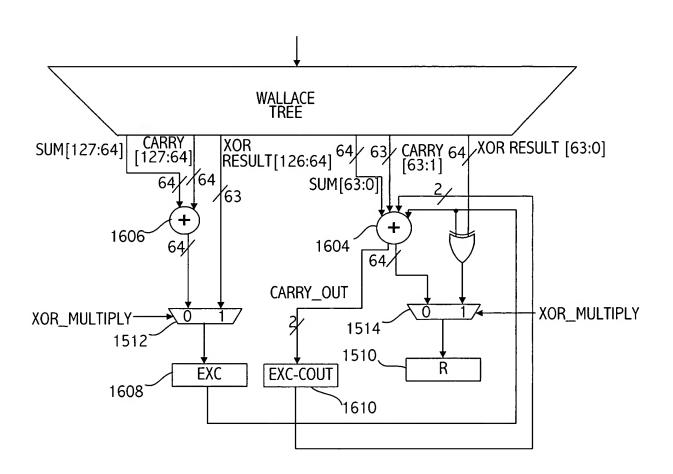


FIG. 16

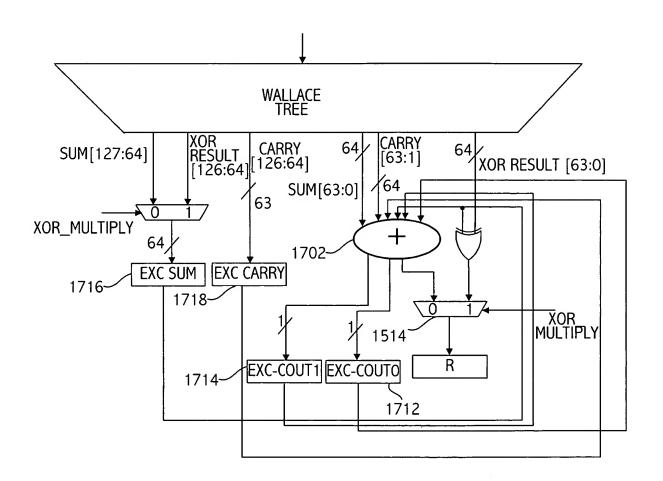
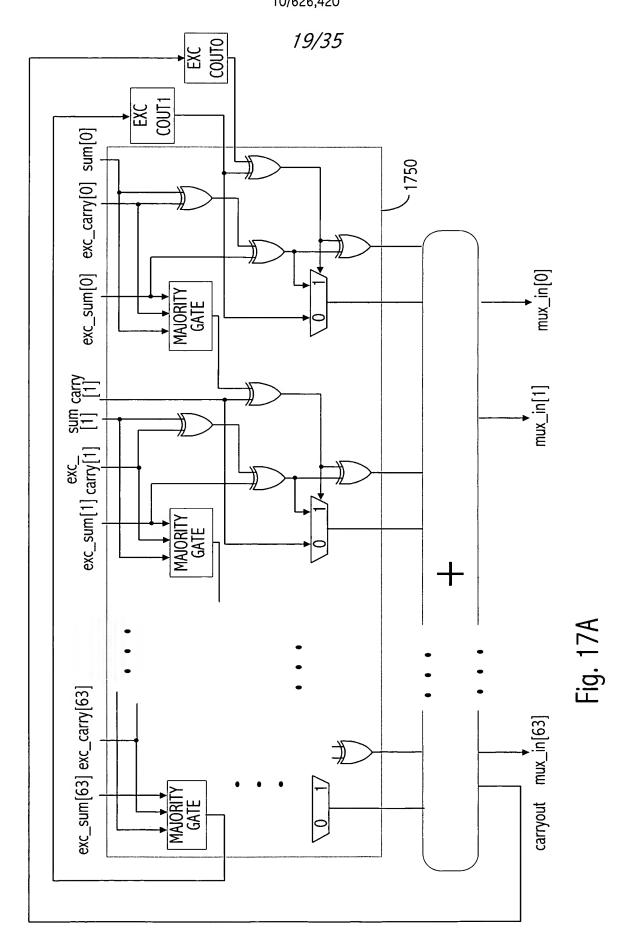


FIG. 17



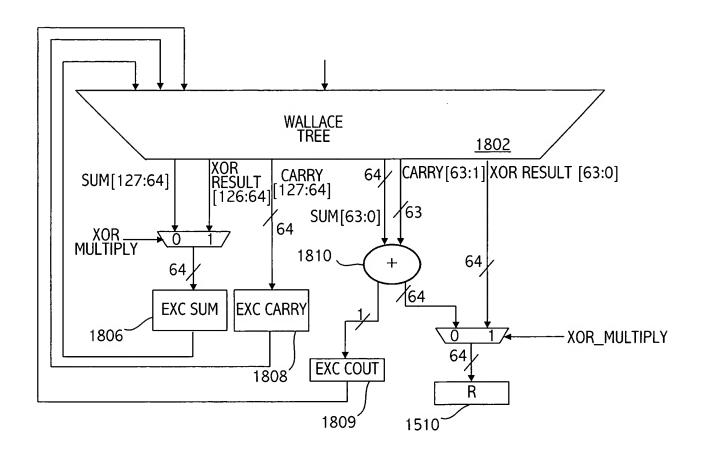


FIG. 18

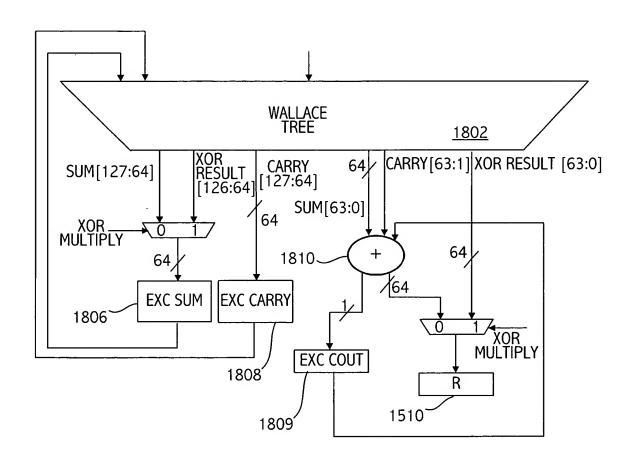


FIG. 19

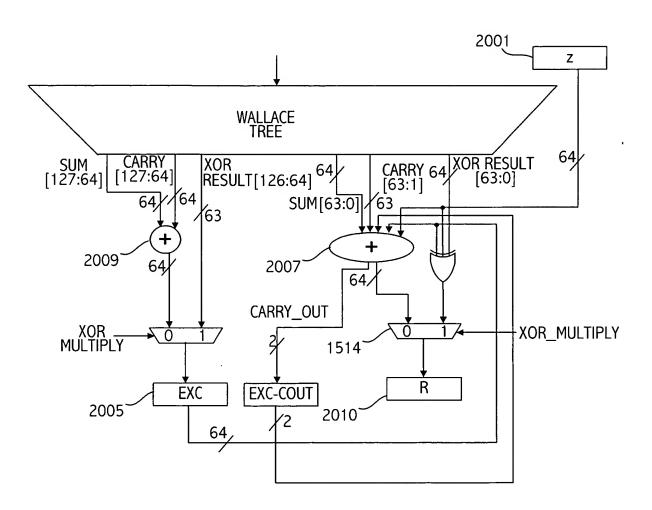
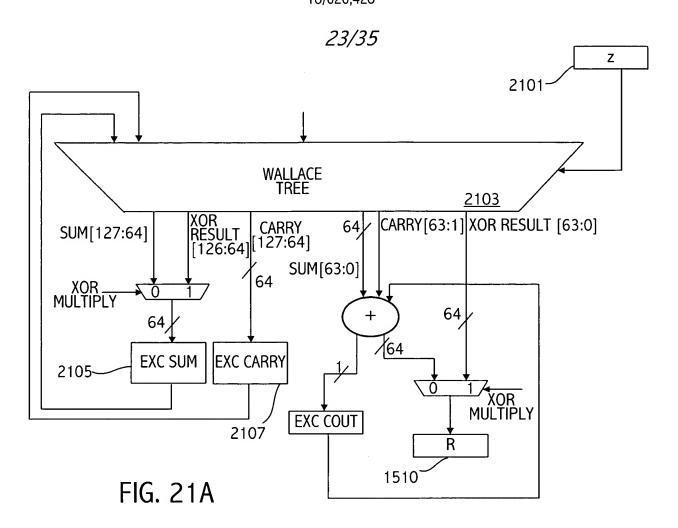
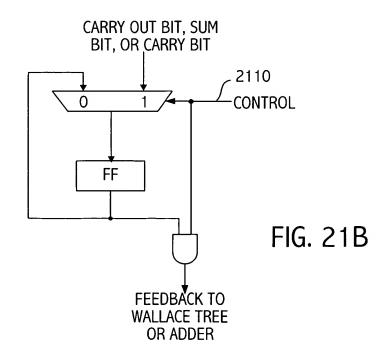


FIG. 20





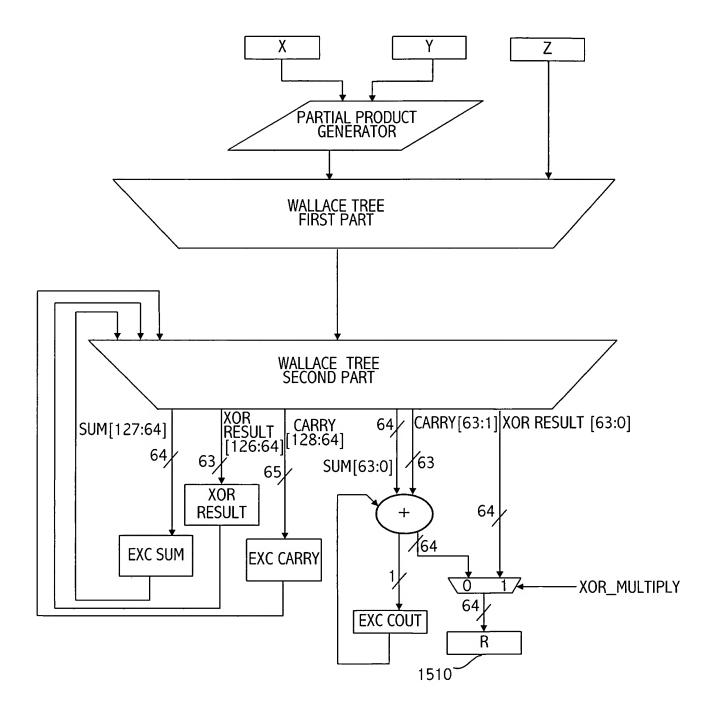


FIG. 21C

25/35

